PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-232775
(43)Date of publication of application : 27.08.1999

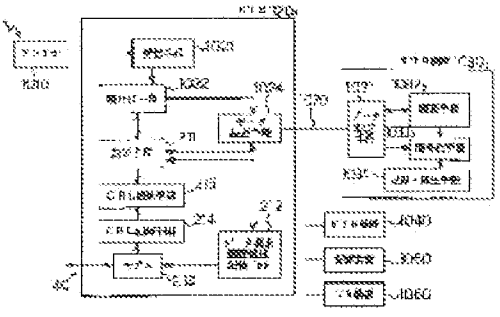
(51)Int.Cl. G11B 20/10

(21)Application number : 10-031846
(22)Date of filing : 13.02.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : YAMADA MASAZUMI
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI

(54) CONTROL STANDARD MAKING METHOD, CONTROL STANDARD MAKING SYSTEM, AND MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable detecting an illegal terminal device before damage occurs more surely than conventional one.
SOLUTION: When data is required from a VTR device 1030 and the like having respective intrinsic EU 164 to STB 120, a certification means 211 performs certification based on the prescribed control standard about their data request, it is decided whether required data is transferred from STB 120 to the VTR device 1030 performing request or not in accordance with the certification result, and a data request history information storing means 212 sends data request history information including EU 164 of the VTR device to a control device 110 in accordance with the certification result. The control device discriminates whether the VTR device 1030 is a regular one or not by the prescribed discrimination standard utilizing the data request history information, makes CRL based on the certification result, and sends it to the SBT 120.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－232775

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ

審査請求　未請求　請求項の数13　ＯＬ　（全 15 頁）

(21)出願番号　特願平10－31846

(22)出願日　平成10年(1998)２月13日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

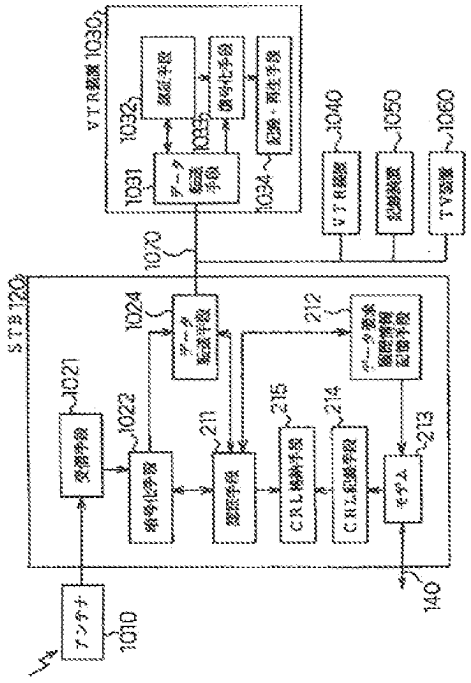
最終頁に続く

(54)【発明の名称】　管理基準作成方法、管理基準作成システム、及び媒体

(57)【要約】

【課題】不正な端末装置を被害発生前に未然に検出出来ないという課題。

【解決手段】それぞれ固有のＥＵＩ６４を有するＶＴＲ装置１０３０等からＳＴＢ１２０に対しデータ要求が有った際、認証手段２１１がそれらのデータ要求に関して、所定の管理基準に基づいた認証を行い、認証の結果に応じて、ＳＴＢ１２０から、要求を行ったＶＴＲ装置１０３０に対して、その要求されたデータを転送するかどうかを決定し、データ要求履歴情報記憶手段２１２が認証の結果に応じて管理装置１１０に対して、そのＶＴＲ装置のＥＵＩ６４を含むデータ要求履歴情報を送り、管理装置１１０は、そのデータ要求履歴情報を利用して、所定の判定基準により、そのＶＴＲ装置１０３０が正規なものであるか否かを判定し、その判定結果に基づいてＣＲＬを作成し、ＳＢＴ１２０に送信する構成。



1

【特許請求の範囲】

【請求項１】　それぞれ固有の識別子を有する各データ要求端末装置からデータ転送装置に対しデータ要求が有った際、それらのデータ要求に関して、所定の認証基準に基づいた認証を行い、

前記認証の結果に応じて、前記データ転送装置から、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定し、

常に、又は前記認証の結果に応じて、前記データ転送装置から管理装置に対して、そのデータ要求端末装置の前記識別子を含むデータ要求履歴情報を送り、

前記管理装置は、前記送られてくるデータ要求履歴情報を利用して、所定の判定基準により、そのデータ要求履歴情報に含まれたデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新することを特徴とする管理基準作成方法。

【請求項２】　前記複数のデータ要求端末装置と前記データ転送装置とにより形成されるグループは複数グループ有り、

前記データ要求履歴情報は、前記識別子の他に、その識別子を有する前記データ要求端末装置からの前記データ要求の有った時刻を特定する時刻情報と、そのデータ要求端末装置の所在を特定する所在情報とを含む情報であり、

前記管理装置における前記所定の判定基準は、前記複数のデータ転送装置から送信されてくる全てのデータ要求履歴情報の中で、同一の識別子が複数存在する場合、それら複数の識別子に対応する前記時刻情報及び前記所在情報をそれぞれ比較して、不正の可能性がある識別子を有するデータ要求端末装置を決定するものであることを特徴とする請求項１記載の管理基準作成方法。

【請求項３】　前記判定基準による判定結果、前記不正の可能性がある識別子を有するデータ要求端末装置が決定された場合、それら同一の識別子を有する全てのデータ要求端末装置を不正なものと見なし、前記管理基準として、それら不正なものと見なされたデータ要求端末装置の不正リストを作成、又は更新することを特徴とする請求項２記載の管理基準作成方法。

【請求項４】　前記管理装置は、前記不正リストの全部又は一部を前記データ転送装置に送信し、

前記データ転送装置は、前記送信されてきた不正リストを少なくとも利用して前記認証を行うことを特徴とする請求項３記載の管理基準作成方法。

【請求項５】　それぞれ固有の識別子を有する各データ要求端末装置に接続されたデータ転送装置を単数又は複数管理する管理装置は、送られてくる、新規に接続される予定の又は新規に接続された前記データ要求端末装置の識別子を含む新規登録情報を利用して、所定の判定基準により、前記新規登録情報に対応するデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新することを特徴とする管理基準作成方法。

2

【請求項６】　前記複数のデータ要求端末装置と前記データ転送装置とにより形成されるグループは複数グループ有り、

前記データ転送装置は、新規に接続された前記データ要求端末装置の前記データ転送装置との接続を検知した際、そのデータ要求装置の新規登録情報を前記管理装置に送信するものであり、

前記所定の判定基準は、前記新規登録情報が送信されてくる度に、その新規登録情報に含まれる識別子と同一の識別子が、前記複数のデータ転送装置から送信されてきて保持されている前記識別子のリストの中に、既に存在しているか否かを判定する基準であることを特徴とする請求項５記載の管理基準作成方法。

【請求項７】　前記判定基準による判定結果が、前記同一の識別子が前記リスト中に存在していることを示す場合、それら同一の識別子を有する全てのデータ要求端末装置を不正なものと見なし、前記管理基準として、それら不正なものと見なされたデータ要求端末装置の不正情報を作成、又は更新することを特徴とする請求項６記載の管理基準作成方法。

【請求項８】　前記判定基準による判定結果が、（１）前記同一の識別子が前記リスト中に存在していることを示す場合、それら同一の識別子を有する全てのデータ要求端末装置を不正なものと見なし、前記管理基準として、それら不正なものと見なされたデータ要求端末装置の不正情報を作成、又は更新し、又、（２）前記同一の識別子が前記リスト中に存在していないことを示す場合、前記新規登録情報に含まれる前記識別子を有するデータ要求端末装置を正規なものと見なし、前記管理基準として、その正規なものと見なされたデータ要求端末装置の正規情報を作成、又は更新することを特徴とする請求項６記載の管理基準作成方法。

【請求項９】　前記管理装置は、前記不正情報の全部若しくは一部を、又は前記正規情報を前記データ転送装置に送信し、

前記データ転送装置は、各データ要求端末装置からデータ要求が有った際、それらのデータ要求に関して、前記送信されてきた不正情報又は正規情報を少なくとも利用して認証し、その認証結果に応じて、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定するものであることを特徴とする請求項８記載の管理基準作成方法。

【請求項１０】　前記管理装置が、前記不正情報の一部を前記データ転送装置に送信する場合、前記不正情報に挙げられているデータ要求端末装置に関する情報の内、そのデータ転送装置と接続関係にあるデータ要求端末装置に対応する情報を抽出し、送信することを特徴とする

請求項４又は９記載の管理基準作成方法。

【請求項１１】　それぞれ固有の識別子を有する複数のデータ要求端末装置と、

それらデータ要求端末装置からデータ要求が有った際、それらのデータ要求に関して、所定の認証基準に基づいた認証を行い、（１）その認証の結果に応じて、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定し、又、（２）常に、又はその認証の結果に応じて、そのデータ要求端末装置の前記識別子を含むデータ要求履歴情報を出力するデータ転送装置と、

前記出力された前記データ要求履歴情報を得て、所定の判定基準により、そのデータ要求履歴情報に含まれたデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新する管理装置と、を備えたことを特徴とする管理基準作成システム。

【請求項１２】　請求項１～１０の何れか一つに記載の各ステップの全部又は一部のステップをコンピュータに実行させるためのプログラムを記録したことを特徴とする媒体。

【請求項１３】　請求項１１に記載の各手段の全部又は一部の手段の機能をコンピュータに実行させるためのプログラムを記録したことを特徴とする媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、管理基準作成方法、管理基準作成システム、及び媒体に関する。

【０００２】

【従来の技術】従来より、衛星放送で送られてくるテレビ番組等を、専用の受信機により受信して、その受信機に接続されたＶＴＲ装置で録画したり、テレビで視聴したりすることが行われている。

【０００３】この場合、放送されてくる映像・音声データの中には、記録が禁止されているものや、１回だけ記録可能とされている条件付きデータがある。従って、これらの条件が守られる為には、この条件を正しく認識して、正規に動作する装置をユーザ側が使用することが前提となる。

【０００４】そこで、専用の受信機から、例えばＶＴＲ装置に対して、１回のみ記録可能なデータを送信する場合、先ず、そのＶＴＲ装置が、上記の様な正規な装置であるかどうかを確認するための認証動作が行われるのが通常である。この認証動作の結果、上記条件を無視した動作を行う不正装置であると判定した場合には、データの送信を行わないものである。

【０００５】以下、図１２を参照しながら、従来の専用受信機と端末装置との構成と、その認証動作を中心に説明する。

【０００６】図１２は、従来の専用受信機と端末装置と

の接続状況及び構成を示すブロック図である。

【０００７】同図に示す様に、アンテナ１０１０は、衛星からの放送電波を受信する手段であり、衛星放送受信機（以下、これを単に、ＳＴＢと呼ぶ）１０２０は、受信した放送電波をＡＶデータに変換する手段である。データ伝送ライン１０７０は、ＳＴＢ１０２０と、以下に述べる各端末装置とを間に設けられたデータ伝送のためのバスラインである。又、端末装置として、ＶＴＲ装置（Ａ）１０３０、ＶＴＲ装置（Ｂ）１０４０、記録装置（Ｃ）１０５０、更にＴＶ装置（Ｄ）が、データ伝送ライン１０７０によりＳＴＢ１０２０と接続されている。

【０００８】次に、同図を参照しながら、ＳＴＢ１０２０の内部構成について更に述べる。

【０００９】即ち、受信手段１０２１は、アンテナ１０１０と直結し、受信したデータの復調を行い、その受信データに施されている放送用スクランブルを解除し、更に、多重化されている受信データを分離する手段である。暗号化手段１０３２は、予め備えた暗号化のためのワークキーＫｗにより、受信手段１０２１から出力されてきたＡＶデータを圧縮状態のまま暗号化する手段である。又、暗号化手段１０２２は、認証手段１０２３から得たサブキーを用いて、ワークキーＫｗを暗号化し、その暗号化したワークキーと、上記暗号化したＡＶデータの双方をデータ入出力手段１０２４を介して、端末装置へ出力するための手段である。尚、ここで、上記の様に暗号化されたワークキーをも端末装置へ送る必要があるのは、端末装置では、転送されてきたＡＶデータを復号化した上で、記録等することを前提としているからである。認証手段１０２３は、ＡＶデータの転送要求をしてきた端末装置との間で、双方の装置が正規の装置であるかどうかを互いに確かめ合うため、所定の秘密関数を利用して認証作業を行い、その結果として、認証相手に対応したサブキーを生成する手段である。又、認証手段１０２３は、あらゆる端末装置が有する固有の全ての秘密関数（Ｓａ，Ｓｂ，Ｓｃ，Ｓｄ，・・，Ｓｎ，・・・）を、それらの識別番号と対応させて保有している。データ転送力手段１０２４は、ディジタル・インタフェースとして知られているＩＥＥＥ１３９４である。データ転送手段１０２４は、リアルタイム性の保証が必要となる映像や音声の様なデータの転送に適したアイソクロナス転送と、その必要のない認証用データやコマンド等の転送に適したアシンクロナス転送の２つの転送を行う手段である。

【００１０】次に、ＶＴＲ装置（Ａ）１０３０の内部構成について、更に述べる。

【００１１】同図に示すとおり、データ転送手段１０３１は、データ転送手段１０２４と同様の手段であり、暗号化されたワークキー及び暗号化されたＡＶデータを受け取る手段である。認証手段１０３２は、固有の秘密関数Ｓａを予め有しており、認証作業の結果として、サブ

5

キーＫｓａを生成して、復号化手段１０３３へ出力する手段である。復号化手段１０３３は、データ転送手段１０３１から得た暗号化されたワークキーをサブキーＫｓａにより復号化してワークキーＫｗを復元し、そのワークキーＫｗにより、暗号化されたＡＶデータを復号化する手段である。記録・再生手段１０３４は、復号化されたＡＶデータを記録し、又、その記録データを再生する手段である。

【００１２】尚、その他の端末装置である、ＶＴＲ装置（Ｂ）１０４０、記録装置（Ｄ）１０５０、ＴＶ装置（Ｄ）１０６０も、記録・再生手段を除き、上記ＶＴＲ装置（Ａ）１０３０の構成と基本的に同じである。但し、各認証手段が予め有する秘密関数は、上記各装置の順番でいえば、Ｓｂ、Ｓｃ、Ｓｄである。従って、各装置と、ＳＴＢ１０２０との認証作業により生成されるサブキーは、上記の順番でいえば、Ｋｓｂ、Ｋｓｃ、Ｋｓｄである。

【００１３】以上の構成において、次に、認証作業の内容を簡単に述べる。

【００１４】例えば、ＶＴＲ装置（Ａ）１０３０からＳＴＢ１０２０に対して、ＡＶデータの転送要求を行う場合、その実行に先立ち次のような認証作業が必要となる。

【００１５】即ち、先ず、ＶＴＲ装置（Ａ）１０３０の認証手段１０３２が、乱数Ａ１，Ａ２を発生させ、これを秘密関数Ｓａにより暗号化する。ここで、暗号化された乱数をＳａ（Ａ１，Ａ２）と記載する。認証手段１０３２は、Ｓａ（Ａ１，Ａ２）と自己の識別番号ＩＤａとをデータ転送手段１０３１を介して、ＳＴＢ１０２０へ転送する（ステップ１００１）。ここで、識別番号は、各端末装置固有の番号で予め与えられている。

【００１６】ＳＴＢ１０２０では、認証手段１０２３がデータ転送手段１０２４を介して、Ｓａ（Ａ１，Ａ２）と識別番号ＩＤａとを得て、その識別番号を認識して、それに対応する秘密関数Ｓａを、保有している複数の秘密関数の中から選択する（ステップ１００２）。これにより、ＳＴＢ１０２０が、ＶＴＲ装置（Ａ）１０３０との間で認証に使用すべき秘密関数が特定される。

【００１７】次に、ＳＴＢ１０２０の認証手段１０２３が、秘密関数Ｓａを用いて、上記受信したＳａ（Ａ１，Ａ２）を解読して、復元したＡ１，Ａ２の内、後者の乱数Ａ２を、暗号化せずにＶＴＲ装置（Ａ）１０３０へ送る（ステップ１００３）。

【００１８】次に、ＶＴＲ装置（Ａ）１０３０の認証手段１０３２が、ＳＴＢ１０２０から送られてきたＡ２と、自らが、上記ステップ１００１で発生させた乱数Ａ２とを比較する。双方が一致すれば、ＳＴＢ１０２０が正規の装置であると判断出来る（ステップ１００４）。

【００１９】次に、ＳＴＢ１０２０側の認証手段１０２３が、乱数Ｂ１，Ｂ２を発生させ、これを秘密関数Ｓａ

6

により暗号化する。そして、Ｓａ（Ｂ１，Ｂ２）をＶＴＲ装置（Ａ）１０３０へ転送する（ステップ１００５）。

【００２０】ＶＴＲ装置（Ａ）１０３０では、認証手段１０３２が秘密関数Ｓａを用いて、上記受信したＳａ（Ｂ１，Ｂ２）を解読して、復元したＢ１，Ｂ２の内、後者の乱数Ｂ２を、暗号化せずにＳＴＢ１０２０へ送る（ステップ１００６）。

【００２１】次に、認証手段１０２３が、ＶＴＲ装置（Ａ）１０３０から送られてきたＢ２と、自らが、上記ステップ１００５で発生させた乱数Ｂ２とを比較する。双方が一致すれば、ＶＴＲ装置（Ａ）１０３０が正規の装置であると判断出来る（ステップ１００７）。

【００２２】以上により、双方が共に正規の装置であることが互いに確認出来き、認証作業が完了し、ＶＴＲ装置（Ａ）１０３０へのＡＶデータの転送が許可される。

【００２３】この認証作業の結果、４つの乱数Ａ１，Ａ２とＢ１，Ｂ２が、双方の装置の認証手段１０２３，１０３２に存在している。そこで、次に、双方の認証手段１０２３，１０３２がそれぞれ、乱数Ａ１，Ｂ１を用いて上記サブキーＫｓａを生成する。尚、サブキーの生成に際し、乱数Ａ２，Ｂ２を使用しないのは、これらは、暗号化せずに転送されたという経緯があるため、その様な経緯の無い乱数Ａ１，Ｂ１を使用する方が、キーの安全性から見て、より優れているからである。

【００２４】暗号化手段１０２２では、この様にして生成されたサブキーＫｓａを用いて、ワークキーＫｗが暗号化され、又、ＡＶデータはワークキーＫｗで暗号化される。そして、上記暗号化されたワークキーＫｓａ（Ｋｗ）と、暗号化されたＡＶデータＫｗ（ＡＶ）の双方がデータ入出力手段１０２４を介して、ＶＴＲ装置（Ａ）１０３０へ出力される。

【００２５】ＶＴＲ装置（Ａ）１０３０では、復号化手段１０３３が、認証手段１０３２から得たサブキーＫｓａを用いて暗号化ワークキーＫｓａ（Ｋｗ）の復号をし、復号されたワークキーＫｗを用いて暗号化ＡＶデータＫｗ（ＡＶ）の復号を行うものである。

【００２６】

【発明が解決しようとする課題】しかしながら、上記の様な認証方法では、不正者が、正規な装置の秘密関数Ｓｎと識別番号ＩＤｎとをそっくりそのまま模倣して、上記と同じ認証方法を行える不正な装置を製造・販売し、その不正装置が使用された場合、上記認証方法では、その装置が不正な装置であることを見破ることが出来ず、ＡＶデータの転送を阻止することが出来なかった。

【００２７】一般に、盗難キャッシュカード等の第３者による不正使用では、そのキャッシュカードの持ち主に対して、直接的被害が顕著に発生する。そのため、不正使用を直ちに阻止することが可能である。これに対して、放送データの受信端末装置として、上記の様な不正

装置が存在していても、関係者に対する被害が表面化し難いという特殊性がある。例えば、コピー禁止のデータを不正にコピーしても、著作権料等が未払いであるというような具体的な被害が表面化することは希であり、仮に表面化したとしても、それまでにはかなりの時間が経過しており、被害は甚大になることも予想される。

【００２８】この様に、従来の認証方法では、被害が明るみに出てからしか対応が出来ないため、認証方法として不完全であるという課題を有していた。

【００２９】本発明は、この様な従来の方法の課題を考慮し、不正な装置の検出を従来に比べてより確実に行える管理基準作成方法、管理基準作成システム、及び媒体を提供することを目的とする。

【００３０】

【課題を解決するための手段】請求項１記載の本発明は、それぞれ固有の識別子を有する各データ要求端末装置からデータ転送装置に対しデータ要求が有った際、それらのデータ要求に関して、所定の認証基準に基づいた認証を行い、前記認証の結果に応じて、前記データ転送装置から、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定し、常に、又は前記認証の結果に応じて、前記データ転送装置から管理装置に対して、そのデータ要求端末装置の前記識別子を含むデータ要求履歴情報を送り、前記管理装置は、前記送られてくるデータ要求履歴情報を利用して、所定の判定基準により、そのデータ要求履歴情報に含まれたデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新する管理基準作成方法である。

【００３１】請求項５記載の本発明は、それぞれ固有の識別子を有する各データ要求端末装置に接続されたデータ転送装置を単数又は複数管理する管理装置は、送られてくる、新規に接続される予定の又は新規に接続された前記データ要求端末装置の識別子を含む新規登録情報を利用して、所定の判定基準により、前記新規登録情報に対応するデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新する管理基準作成方法である。

【００３２】請求項１１記載の本発明は、それぞれ固有の識別子を有する複数のデータ要求端末装置と、それらデータ要求端末装置からデータ要求が有った際、それらのデータ要求に関して、所定の認証基準に基づいた認証を行い、（１）その認証の結果に応じて、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定し、又、（２）常に、又はその認証の結果に応じて、そのデータ要求端末装置の前記識別子を含むデータ要求履歴情報を出力するデータ転送装置と、前記出力された前記データ要求履歴情報を得て、所定の判定基準により、そのデータ要求履歴情報に含まれたデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新する管理装置とを備えた管理基準作成システムである。

【００３３】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【００３４】（第１の実施の形態）図１は、本発明の一実施の形態における管理基準作成システムの構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の管理基準作成システムの構成について述べる。尚、本実施の形態では、図１２で説明したものと、基本的に同じ構成のものには、同じ符号を付し、その詳細な説明は省略した。

【００３５】図１に示す様に、管理装置１１０は、各地に存在する第１ＳＴＢ１２０，・・・，第ｎＳＴＢ１３０及び各端末装置を管理する装置である。又管理装置１１０は、各ＳＴＢが認証作業において利用するための不正装置リストを作成し、配信する手段である。電話回線１４０は，管理装置１１０と各ＳＴＢ１２０，１３０との間のデータ伝送に利用する手段である。本実施の形態では，第１ＳＴＢ１２０は北海道のＡさん宅に、又、第ｎＳＴＢは沖縄のＮさん宅に設けられているとする。

【００３６】又、各ＳＴＢ１２０，１３０には、データ伝送ライン１０７０上で、端末装置がそれぞれ接続されている。即ち、同図に示す通り、第１ＳＴＢ１２０には、ＶＴＲ装置１０３０、ＶＴＲ装置１０４０、記録装置１０５０）、及びＴＶ装置１０６０が接続されており、又、第ｎＳＴＢ１３０には、ＶＴＲ装置１５０、記録装置１６０、及びＴＶ装置１７０が接続されている。ここで、ＶＴＲ装置１５０が不正装置であるとする。この不正装置は，後述するライセンスキー及びＥＵＩ６４として、正規のＶＴＲ装置１０３０のものをそっくりそのまま模倣することにより不正に製造された装置であるものとする。

【００３７】尚、これら、各端末装置は、図１２にて説明した通り、データ転送手段１０３１としてＩＥＥＥ１３９４を備えている。又、本実施の形態では、これら端末装置は，それぞれＩＥＥＥ１３９４におけるＥＵＩ６４を、各装置固有の番号、即ち、識別番号として予め備えている。ここで、ＥＵＩ６４は，６４ビットの識別コードである。又、これら端末装置は、その識別番号に対応したライセンスキーを備えている。このライセンスキーは，正規の端末装置にのみ与えられる非公開の秘密鍵であるが、ＥＵＩ６４の識別番号は、データ転送等に際し、誰でも知り得るいわゆるＩＤ番号である。以下、ＥＵＩ６４の識別番号を単に、ＥＵＩ６４，又はＩＤ番号と呼ぶ。尚、各ＳＴＢ１２０，１３０についても、固有のＥＵＩ６４が設けられている。これら識別番号は各装置に対して、一対一に対応しており、重複することはない。

【００３８】次に、図２を参照しながら、ＳＴＢ１２０の内部構成について、更に詳細に述べる。

【００３９】図２に示す通り、ＳＴＢ１２０は、図１２で述べた認証手段１０２３の構成に加えて、データ要求履歴情報記憶手段２１２、モデム２１３、ＣＲＬ記録手段２１４、及びＣＲＬ格納手段２１５を備える。

【００４０】認証手段２１１は、ライセンスキーと同じキーであるサービスキーを作ることが出来るサービスキー生成関数を備えている点と、認証において、後述する不正装置のリストを参照する点で、図１２で述べた認証手段１０２３と相違する。このサービスキー生成関数は、端末装置から得られたＥＵＩ６４（ＩＤ番号）から、サービスキーを生成する関数である。そのため、認証手段２１１は、端末装置のＥＵＩ６４を予め記憶しておく必要がない。

【００４１】データ要求履歴情報記憶手段２１２は、端末装置から所定の放送番組のデータ転送要求があった場合、後述する認証作業を経て、要求データの転送が完了したものについて、そのデータ要求に関する履歴情報を生成し、その都度記憶する手段である。このデータ要求履歴情報は、データ転送要求をした端末装置のＥＵＩ６４と、その端末装置からのデータ要求の有った時刻を特定する時刻情報と、その端末装置の所在を特定する所在情報とから構成されている。尚、データ要求履歴情報記憶手段２１２は、これらＥＵＩ情報～所在情報を認証手段２１１から得る。又、データ要求履歴情報記憶手段２１２は、１ヶ月間の各端末装置からのこのような履歴情報を蓄積しておき、１ヶ月毎に、モデム２１３を介して、管理装置１１０へ送る手段である。

【００４２】又、ＣＲＬ記録手段２１４は、管理装置１１０から送られてくる不正装置を記載したリストデータをモデム２１３から得て、ＣＲＬ格納手段２１５に記録・更新する手段である。ＣＲＬ格納手段２１５は、不正装置のリストデータを格納するためのメモリ手段である。尚、本明細書では、不正装置のリストを、単にＣＲＬ（Certification Revocation List）と呼ぶ。又、請求項１記載の本発明の管理基準は、ＣＲＬに対応する。

【００４３】次に、図３を参照しながら、管理装置１１０の内部構成について、更に詳細に述べる。

【００４４】図３に示す通り、履歴情報記憶手段１１２は、モデム１１１を介して、各ＳＴＢ１２０，１３０から１ヶ月毎に同時期に送信されてくる各データ要求履歴情報を、送信元のＳＴＢのＥＵＩ６４と対応させて、一時的に記憶する手段である。不正装置決定手段１１３は、上記履歴情報記憶手段１１２に記憶されている各ＳＴＢからの１ヶ月分の全てのデータ要求履歴情報の中で、同一のＥＵＩ６４が複数存在する場合、それら複数のＥＵＩ６４に対応する時刻情報及び所在情報をそれぞれ比較して、不正の可能性があるＥＵＩ６４を有するデータ要求端末装置を決定する手段である。ＣＲＬ作成手段１１４は、不正装置決定手段１１３から１ヶ月毎に出力される上記決定結果を得て、不正装置のリストを作成し、出力する手段である。全ＣＲＬ記憶手段１１５は、ＣＲＬ作成手段１１４からのリストデータを得て、既に蓄積されているリストに対し、新たな不正装置の追加や、データの修正等を行い、全ての地域の端末装置に関する全ＣＲＬを記憶する手段である。個別ＣＲＬ作成手段１１６は、各ＳＴＢに対応した個別のＣＲＬを作成し、モデム１１１を介して、対応するＳＴＢに送信する手段である。個別のＣＲＬは、ＳＴＢ毎にまとめられた不正装置のリストであり、不正装置が検出されていないＳＴＢについては作成されない。

【００４５】以上の構成において、次に、主に図４～図６（ｃ）を参照しながら、本実施の形態の動作を述べ、同時に本発明の管理基準作成方法に係る一実施の形態についても説明する。尚、図４は、１９９７年１月１日から、同月３１日までの、ＳＴＢ１２０におけるデータ要求履歴情報記憶手段２１２の記憶内容を説明する図であり、図５は、１９９７年１月１日から、同月３１日までの、管理装置における履歴情報記憶手段１１２の記憶内容を説明する図である。

【００４６】ここでは、１９９７年１月３１日の時点では、ＳＴＢ１２０のＣＲＬ格納手段２１５のＣＲＬ（不正装置のリスト）には、不正装置は未だ記載されていない、即ち、空の状況であるとする。又、ＳＴＢ１３０のＣＲＬ格納手段のＣＲＬについても、空の状態である。

【００４７】又、ここでの説明は、先ず、（１）ＳＴＢにおける、ＣＲＬを利用した認証動作について述べ、次に、（２）管理装置におけるＣＲＬの作成及び、ＳＴＢへのＣＲＬの配信について述べ、最後に、（３）ＳＴＢにおける、ＣＲＬの更新動作を述べる。

（１）ＳＴＢにおける、ＣＲＬを利用した認証動作：ここでは、ＳＴＢ１２０が、受信手段１０２１により受信した放送番組のＡＶデータについて、例えば、正規の装置であるＶＴＲ装置１０３０からの転送要求を受けた場合、次のような認証動作を行う。尚、この転送要求は、図４、図５中に記載されている履歴情報の内、平成１０年１月１０日午前１２時１０分にあった要求に対応している。

【００４８】ステップ１：先ず、ＳＴＢ１２０の認証手段２１１は、転送要求をしてきたＶＴＲ装置１０３０のＥＵＩ６４（ここでは、１１０３０番とする）をデータ転送手段１０２４から得る。

【００４９】ステップ２：そして、認証手段２１１は、ＣＲＬ格納手段２１５のＣＲＬを参照して、そのＥＵＩ６４と同じ番号が不正装置の番号としてＣＲＬの中に登録されていないかどうかをチェックする。この時点では、上記の通り、ＣＲＬは空の状態であるため、そのＥＵＩ６４は未登録であるとの判定結果が出て、本格的な認証作業に入る（ステップ３）。尚、このチェック段階

で、ＣＲＬに登録されているとの判定が出ると、その後の認証作業は行わず、要求のあったデータの転送も行わない。

【００５０】ステップ３：認証手段２１１は、ステップ１で得たＶＴＲ装置１０３０のＥＵＩ６４を用いて、サービスキー生成関数からサービスキーを生成する。この様にして生成されたサービスキーは、ＶＴＲ装置１０３０が有するライセンスキーと同一の鍵である。尚、ライセンス一及びサービスキーは、図１２で述べた秘密関数Ｓａに対応する。

【００５１】認証手段２１１は、この様にして生成したサービスキーを用いて、一方、ＶＴＲ装置１０３０は、予め備えているライセンスキーを用いて、双方の間で、図１２で既に説明したものと同様の認証作業を行う。即ち、双方の装置が、それぞれ乱数Ａ１，Ｂ１を用いて、同一のサブキーＫｓａを生成する。

【００５２】ステップ４：暗号化手段１０２２は、上記サブキーＫｓａを用いて、ワークキーＫｗを暗号化し、且つ、ワークキーＫｗを用いて、ＡＶデータを暗号化し、それら双方の暗号化データ（Ｋｓａ（Ｋｗ），Ｋｗ（ＡＶ））をＶＴＲ装置１０３０へ転送する。

【００５３】尚、この認証の過程で、例えば、端末装置から送られてきたＥＵＩ６４が、その端末装置が有するライセンスキーと予め定められた対応関係を有していない、全くでたらめな番号であるとすると、サービスキー生成関数により生成された鍵は、そのライセンスキーとは一致しなくなる。というのは、サービスキー生成関数は、上記予め定められた対応関係に基づいて、ＥＵＩ６４からサービスキーを生成するように構成されているからである。従って、この場合、双方の装置の有するキーが同一であることを前提とした上記認証は成立しなくなり、この場合、要求されたデータの転送は行われない。

【００５４】ステップ５：データ要求履歴情報記憶手段２１２は、ステップ４にてデータ転送が完了したものに関して、認証手段２１１から、その転送先であるＶＴＲ装置１０３０のＥＵＩ６４として、１１０３０番と、要求の有った時刻情報として、平成１０年１月１０日午前１２時１０分のそれぞれの情報を得て、データ要求履歴情報として記録する（図４参照）。ここで、図４の記載について説明する。即ち、同図において、端末装置のＥＵＩ６４の欄４０１に記載された各番号としての、３１０６０番，１１０４０番，１１０３０番，及び２１０５０番は、前から順に、ＴＶ装置１０６０、ＶＴＲ装置１０４０、ＶＴＲ装置１０３０，そして記録装置１０５０のＥＵＩ６４を示している。

【００５５】ステップ６：各端末装置１０３０～１０６０からデータ転送要求が有る毎に、上記ステップ１～５を上記と同様に実行する。そして、データ要求履歴情報記憶手段２１２は、１ヶ月間に記録蓄積された各履歴データ（図４参照）に、ＳＴＢ１２０のＥＵＩ６４（ここでは、９０００１番とする）及びその所在情報としての電話番号を添えたものをデータ要求履歴情報として（モデム２１３から電話回線１４０を介して、１ヶ月毎に管理装置１１０へ転送する。

（２）管理装置におけるＣＲＬの作成及び，ＳＴＢへのＣＲＬの配信動作：ここでは、管理装置１１０の動作を述べる。

【００５６】ステップ１０１：管理装置１１０の履歴情報記憶手段１１２には、各地のＳＴＢ１２０～１３０から１ヶ月毎に上述したデータ要求履歴情報がモデム１１１を介して転送されてくる。履歴情報記憶手段１１２は、これらの情報を履歴情報として保持する。

【００５７】ステップ１０２：不正装置決定手段１１３は、履歴情報記憶手段１１２に保持された履歴情報を得て、その時刻情報により、データ内容を時間順に並べ替える（図５参照）。図５は、並べ替えられた履歴情報の内容を説明するための図である。

【００５８】そして、端末装置のＥＵＩ６４の欄５０１（図５参照）に示す端末装置のＥＵＩ６４が同一のものがあれば、それらに対応する時刻情報及び所在情報をそれぞれ比較して、不正の可能性があるＥＵＩ６４に対応する端末装置を決定する。

【００５９】即ち、図５に示す場合、符号５１１，５１２，５１３の付された各行に記載された端末装置のＥＵＩ６４が、全て１１０３０番である。そこで，これらが先ずチェックされる。符号５１１と５１２の付された行の時刻情報同士を比較するとそれぞれ異なる時刻における転送要求の履歴であり、双方の履歴に矛盾はないと判断できる。しかし、符号５１２と５１３を付した行に記載された２つの履歴は、同一のＥＵＩ６４を有する装置は存在しないという前提と矛盾する状況が発生していることを示している。尚、図５のＳＴＢのＥＵＩ６４の欄５０４に記載された番号９０００２は、ＳＴＢ１３０のＥＵＩ６４である。

【００６０】即ち、不正装置決定手段１１３は、これら双方の時刻情報の欄５０２及び所在情報の欄５０３のデータを比較した際、一方は沖縄、他方は北海道という地理的に遠く離れた場所から、１０分違いで、同一のＥＵＩ６４を有する装置により転送要求が有ったという事実から見て、同一のＥＵＩ６４を有する装置が，北海道のＡさん宅と、沖縄のＮさん宅に存在すると判断する。そして、不正装置決定手段１１３は、これら双方の装置の双方ともが不正な装置であると見なし、その判定結果をＣＲＬ作成手段１１４へ送る。尚、沖縄のＮさん宅に設置されているＶＴＲ装置１５０が現実に不正な装置であるとしたが、この段階では、何れが現実に不正な装置であるのかというところまでは、分からないので、とりあえず双方を不正と見なすものである。尚、何れが不正であるかの判定については、後述する。又、符号５２１，５２２を付した行に記載された履歴データを比較した結

果からは、同一のＥＵＩ６４を有する装置は存在しないという前提と矛盾する状況は見あたらない。

【００６１】ステップ１０３：ＣＲＬ作成手段１１４は、不正装置決定手段１１３から得られた判定結果から、図６（ａ）に示す様なＣＲＬを作成して、全ＣＲＬ記憶手段１１５へ送る。この様な、ＣＲＬの作成動作は、毎月行われ、その度に、全ＣＲＬ記憶手段１１５に記憶する。従って、全ＣＲＬ記憶手段１１５は、ＣＲＬ作成手段１１４から送られてくるリストにより、既に記憶しているＣＲＬに追加、訂正などを加えて、その都度、更新するものである。

【００６２】ステップ１０４：個別ＣＲＬ作成手段１１６は、ＣＲＬ作成手段１１４で作成されたＣＲＬにおけるＳＴＢのＥＵＩ６４の欄６０１を見て、そのＣＲＬの内容をＳＴＢ毎に分離する。図６（ｂ），（ｃ）は、それぞれ、ＳＴＢ１３０，ＳＴＢ１２０に配信する為に作成された個別ＣＲＬである。個別ＣＲＬ作成手段１１６は、これらの個別リストを対応するＳＴＢへ、モデム１１１を介して配信する。

（３）ＳＴＢにおける、ＣＲＬの更新動作：管理装置１１０から配信されてきた個別ＣＲＬ（図６（ｃ）参照）を得た、ＳＴＢ１２０は、次の様な動作を行う。

【００６３】ステップ２０１：即ち、ＣＲＬ記録手段２１４は、モデム２１３から上記個別ＣＲＬを得て、それまで空の状態であったＣＲＬ格納手段２１５に記録する。これによりＣＲＬ格納手段２１５には、ＳＴＢ１２０に接続されているＶＴＲ装置１０３０（ＥＵＩ６４が１０３０番）が不正装置として登録される。従って、今後、このＶＴＲ装置１０３０からのデータ転送要求が有っても、上記ステップ２の段階で不正装置であることが判明するので、データ転送は行われない。これにより、不正装置による被害の拡大が防止出来る。尚、ＳＴＢ１３０においても、全く同様の動作が行われる。この場合は、ＳＴＢ１３０のＣＲＬ格納手段には、ＶＴＲ装置１５０（ＥＵＩ６４が１１０３０番）が不正装置として登録される。

【００６４】（第２の実施の形態）図７，８は、本発明の一実施の形態における管理基準作成システムを構成するＳＴＢ及び管理装置の構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の管理基準作成システムの構成について述べる。尚、本実施の形態では、第１の実施の形態で説明したものと、基本的に同じ構成のものには、同じ符号を付し、その詳細な説明は省略した。又、本実施の形態のシステム全体の構成は、基本的に図１で述べたものと同じである。

【００６５】本実施の形態と上記実施の形態の主な相違点は、端末装置についての不正・正規判定情報の作成のプロセスである。従って、ここでは、この相違点を中心に説明する。尚、請求項５に記載の本発明の管理基準は、不正・正規判定情報に対応する。

【００６６】図７に示すＳＴＢ１２０の構成において、図２で示した構成と相違する主な点は、新規接続装置検出手段７１１と、不正・正規情報格納手段７１２と、不正・正規情報記録手段７１３が、図２のデータ要求履歴情報記憶手段２１２，ＣＲＬ格納手段２１５と、ＣＲＬ記録手段２１４の代わりに設けられていることである。更に、認証手段７１４は、第１の実施の形態で述べたものとは異なり、端末装置からのデータ転送要求に関する履歴情報を出力する構成にはなっていない。尚、その他の構成は、同じである。

【００６７】新規接続装置検出手段７１１は、ＳＴＢ１２０のデータ伝送ライン１０７０に新たに接続された装置が有った場合、それを検出し、そのＥＵＩ６４を取得する手段である。取得したＥＵＩ６４は、ＳＴＢ１２０のＥＵＩ６４を添えて、モデム２１３から、管理装置１１０へ送られる。この動作は、新に接続された装置の管理装置への新規登録のための作業であり、同時に、その新規接続装置が不正でないかどうかを確認するための作業でもある。尚、この動作は、新規登録の際に行うものであるから、上記第１の実施の形態で述べたデータ転送要求の度に行うものとは異なり、初回のみの動作である。

【００６８】不正・正規情報記録手段７１３は、管理装置１１０から送られてくる情報を不正・正規情報格納手段７１２に格納する手段である。

【００６９】次に、図８を参照しながら、管理装置１１０の構成を述べる。

【００７０】同図に示すように、照会手段８１１は、ＳＴＢ１２０～１３０から送られてくる、新規登録情報としての、新設された端末装置のＥＵＩ６４とその送信元のＳＴＢのＥＵＩ６４とを得て、それが不正であるかどうかを判定する手段である。新規登録装置一覧情報記憶手段８１２は、照会手段８１１から得た新規登録装置のＥＵＩ６４を記憶する手段である。

【００７１】又、不正・正規判定情報作成手段８１３は、照会手段８１１による上記チェック結果から新規登録のあった装置について、不正であるか、あるいは正規であるかの判定情報を作成し、その何れかの情報をモデム１１１を介して、対応するＳＴＢに送信する手段である。尚、不正・正規判定情報作成手段８１３は、重複登録となった場合、そのＥＵＩ６４を有する双方の装置を不正装置と見なし、ＳＴＢ毎に対応する不正情報のリスト（図６（ｂ），（ｃ）参照）を作成し、配信するものである。

【００７２】以上の構成において、次に、主に図９（ａ）～図１０（ｂ）を参照しながら、本実施の形態の動作を述べ、同時に本発明の管理基準作成方法に係る一実施の形態についても説明する。尚、説明の都合上、本実施の形態では、図１に示すＶＴＲ装置１０４０、記録装置１０５０、及びＴＶ装置１０６０は、既にＳＴＢ１

15

２０に接続済であり、又、ＶＴＲ装置１５０、記録装置１６０、及びＴＶ装置１７０は、既にＳＴＢ１３０に接続済であり、これらの端末装置については、以下に説明する新規登録も済んでいるものとする。又、ＶＴＲ装置１０３０は、ＳＴＢ１２０に対して、新たに接続される装置であるとする。尚、ＶＴＲ装置１５０は、上記実施の形態でも説明した通り、不正装置であるとする。ここでの説明は、先ず、（１）ＳＴＢにおける、新規に接続される装置の検出動作について述べ、次に、（２）管理装置における、新規登録及び不正・正規判定情報の作成等について、最後に、（３）ＳＴＢにおける、不正・正規判定情報の更新及び、不正・正規判定情報を利用した認証動作について述べる。尚、これらの説明は、第１の実施の形態との相違点を中心に行う。

（１）ＳＴＢにおける動作：上述の通り、ＳＴＢ１２０に対し、ＶＴＲ装置１０３０が、新たに接続されたとする（図７参照）。

【００７３】ステップ２０１：図７に示す新規接続装置検出手段７１１は、データ伝送ライン１０７０に接続されている全ての端末装置のＥＵＩ６４を、定期的に読み出し、内蔵するメモリ（図示省略）に記録する。そして、既に記録されている端末装置のＥＵＩ６４の最新の記録データと比較する。

【００７４】ＶＴＲ装置１０３０が新たに接続された状況では、上記ＥＵＩ６４の定期的な読み出し、及び上記比較動作により、ＥＵＩ６４が１１０３０番の装置が、新規に接続されたことが検出出来る。

【００７５】ステップ２０２：更に、新規接続装置検出手段７１１は、上記検出した新規登録の対象となる装置のＥＵＩ６４（１１０３０番）と、送信元のＳＴＢ１２０のＥＵＩ６４（９０１２０番）とを新規登録情報として、モデム２１３を介して管理装置１１０へ送信する。

（２）管理装置における動作：図９（ａ）は、ＶＴＲ装置１０３０が登録される以前の、新規登録装置一覧情報記憶手段８１２の記憶内容を説明するための図であり、図９（ｂ）は、ＶＴＲ装置１０３０が登録された後の図である。これらの図面を参照しながら、説明する。

【００７６】ステップ３０１：図８に示す照会手段８１１は、ＳＢＴ１２０から送信されてきた新規登録情報を元に、新規登録装置一覧情報記憶手段８１２の記憶内容（図９（ａ）参照）を調べ、その登録が、重複登録という状況を生じさせないかどうかをチェックする。新規登録情報に含まれているＥＵＩ６４は１１０３０番であり、これは、図９（ａ）に示す通り、既に登録済のもの（図９（ａ）中、符号９０１を付した）と重複する。従って、照会手段８１１は、重複した双方のＥＵＩ６４について、不正であると判定し、出力する。

【００７７】ステップ３０２：新規登録装置一覧情報記憶手段８１２は、照会手段８１１から送られてくる新規登録情報の内容を登録（図中、符号９０２を付した）する。更に、上記判定結果から、重複した双方のＥＵＩ６４について、備考欄９０３に、不正である旨の情報を記録する。尚、何れが本当に不正であるのかの判定については、後述する。

16

【００７８】ステップ３０３：不正・正規判定情報作成手段８１３は、照会手段８１１から送られてくる判定結果から、図１０（ａ），（ｂ）に示すような、不正・正規判定情報のリストを作成する。これらリストは、ＳＴＢ毎にまとめられている。図１０（ａ）、（ｂ）では、上述の通り、判定結果の欄１０１に、不正を示す情報が記録されている。但し、ステップ３０１における、照会手段８１１による新規登録情報の判定の結果、それが正規であると判定された場合，判定結果の欄１０１には、言うまでもなく正規を示す情報が記録される。

【００７９】ステップ３０４：不正・正規判定情報作成手段８０３は、上記のようにして作成した判定結果の個別リストをモデム１１１を介して、ＳＴＢ１２０とＳＴＢ１３０とに送信する。この送信は、上述した新規登録情報がＳＴＢから送られてくる度に実行される。

【００８０】（３）ＳＴＢにおける動作：図１１（ａ）は、不正・正規情報格納手段７１２に既に格納されている内容を示す図であり、図１０（ａ）に示す判定結果の個別リストが送信される以前の状況を示している。又、図１１（ｂ）は、図１０（ａ）に示す判定結果の個別リストの内容が反映された後の状況を示している。

【００８１】図７に示す不正・正規情報記録手段７１３は、管理装置１１０から送信されてきた判定結果の個別リストをモデム２１３から得て、それを図１１（ａ）に示す記録内容に対して追加する。図１１（ｂ）の上から第４行目（図中、符号１１１３を付した）に、上記個別リストの内容が追加されている。同図の判定結果の欄１１１１は、登録端末装置のＥＵＩ６４の欄１１１２に示した装置が不正であるか正規であるかを示している。

【００８２】一方、ＳＴＢ１３０においても、上記と全く同様の動作が行われる。

【００８３】次に、ＶＴＲ装置１０３０から、ＳＴＢ１２０に対して、ＡＶデータの転送要求が有った場合について述べる。

【００８４】この場合は、第１の実施の形態で述べたステップ１～ステップ４で述べた認証動作において、上記ステップ２の内容のみが異なるので、その相違点のみ述べる。

【００８５】即ち、上記ステップ１と同様の動作の後、認証手段７１４は、不正・正規情報格納手段７１２を参照して、転送要求を出した端末装置のＥＵＩ６４が正規であるか不正であるかをチェックする。図１１（ｂ）に示す通り、符号１１１３を付した行に記録された情報によると、上記転送要求をしてきたＥＵＩ６４が１１０３０番の装置は、不正であることが示されている。従って、認証手段７１４は、その後の認証作業は行わず、要

求のあったデータの転送も行わない。

【００８６】尚、チェックの結果、正規である場合、上記ステップ３～４で述べた内容と同様の動作を行う。

【００８７】又、転送要求の有った装置のＥＵＩ６４が、不正・正規情報格納手段７１２に未登録の場合、認証手段７１４は、新規接続装置検出手段７１１に対して、その要求元の装置の新規登録情報を管理装置１１０へ送るように指示する。、これにより、不正装置による被害の拡大が防止出来る。

【００８８】ところで、上述した通り、双方の装置が不正であると判定された場合、その何れが本当に不正であるのかの判定について述る。

【００８９】この場合、ＳＴＢにより不正であると見なされて、要求したデータを転送してもらえなかった使用者は、その不正判定を受けた装置の疑いをはらすため、管理装置１１０を所有する管理センターに、調査を依頼することが可能である。調査依頼を受けた管理センターは、その装置の真偽を調査して、不正な方法により製造又は改造されたものでないかどうかを確実にチェックする。そして、正規であると判明すれば、管理装置に記録されているデータを修正し、その修正結果を該当するＳＴＢへ転送する。これにより、正規であると判明した装置に対しては、転送要求に応じることとなる。

【００９０】又、以上述べた実施の形態の何れか一つに記載の各ステップ（又は手段）の全部又は一部のステップ（手段）をコンピュータに実行させるためのプログラムを記録した磁気記録媒体や光記録媒体などを作成し、これを利用して上記と同様の動作を実行させることも出来る。この場合も上記と同様の効果を発揮する。

【００９１】尚、上記実施の形態では、端末装置から有った全てのデータ転送要求を対象として、データ要求履歴情報記憶手段２１２に記録する場合について述べたが、これに限らず例えば、重要なデータの転送要求のみを対象として、記録する構成でも良い。ここで、重要なデータとしては、例えば、記録したら課金するといったペーパレック（ＰＲＥＣ）やペーパービュー（ＰＰＶ）の様なデータである。従って、例えば、チェンネル毎にお金を支払うものや、無料のチャンネルの番組データなどは、対象外としても良い。

【００９２】又、上記第２の実施の形態では、端末装置が新規接続されたことを自動的に検出する場合について述べたが、これに限らず例えば、新規に購入した装置に登録はがきを添付しておき、使用者が、そのはがきを管理装置を所有する管理センターに送る構成としても良い。

【００９３】又、上記実施の形態では、ＣＲＬや不正・正規情報のＳＴＢへの送信を電話回線を用いて行う場合について述べたが、これに限らず例えば、放送によって送っても良い。

【００９４】又、上記第２の実施の形態では、ＳＴＢ側から送られてきた新規登録情報と、既に送られてきた新規登録情報の蓄積データとを比較して、重複が無いかどうかをチェックする場合について述べたが、これに限らず例えば、装置を製造した各社から送られてくる生産情報に記載された、生産済の正規装置のＥＵＩ６４の一覧データを保持したメモリを備え、上記比較の際、そのメモリの内容との比較も行う構成でも良い。新規登録情報に含まれたＥＵＩ６４が全くでたらめである場合でも、上記メモリの内容と比較することにより、少なくとも生産済の正規装置のＥＵＩ６４とも一致しない様な番号であれば、たとえ新規登録装置一覧情報記憶手段８１２に記録されておらず、重複しない状況であったとしても、不正であると判定出来、不正防止の効果がより向上する。

【００９５】又、上記実施の形態では、本格的な認証動作を行う場合について述べたが、これに限らず例えば、認証内容として、ＣＲＬを参照するのみ、あるいは、不正・正規情報を参照するのみでもかまわない。

【００９６】又、上記実施の形態の各手段の処理動作は、コンピュータを用いてプログラムの働きにより、ソフトウェア的に実現してもよいし、あるいは、上記処理動作をコンピュータを使用せずに特有の回路構成により、ハード的に実現してもよい。

【００９７】又、本願発明のデータ転送装置は、上記実施の形態では、ＳＴＢであり、そのＳＴＢは、新規に接続されたデータ要求端末装置のＳＴＢとの接続を検知した際、そのデータ要求装置の新規登録情報を管理装置に送信する場合について説明したが、これに限らず例えば、新規接続装置検出手段７１１は、ＶＴＲ装置１０３０から新たに認証を要求された際に、そのＶＴＲ装置１０３０のＥＵＩ６４を得て、既に新規接続を確認して記録されている端末装置のＥＵＩ６４と比較して、同一のものがなければ、そのＶＴＲ装置１０３０が、新規に接続されたものとして検出する構成でもよい。

【００９８】又、上記実施の形態では、認証の結果、正規な装置であることが確認できた場合に、データ転送装置（ＳＴＢ）から管理装置に対して、そのデータ要求端末装置の識別子（ＥＵＩ６４）を含むデータ要求履歴情報を送るという例を説明したが、これに限らず例えば、認証の結果に関わらず、管理装置に対して、そのデータ要求履歴情報を送る構成でもよい。この場合、認証の過程で、不正な装置であると判明した場合には、その旨も履歴情報と共に送ればよい。

【００９９】又、上記実施の形態では、ＳＴＢが認証動作の中で、本願発明の管理基準（ＣＲＬ又は、不正・正規判定情報）を利用する場合について述べたが、これに限らず例えば、ＳＴＢとしては、その認証動作において、上記ＣＲＬや不正・正規判定情報を使用しない構成でも良い。

【０１００】

19

【発明の効果】以上述べたところから明らかなように本発明は、不正な装置の検出を従来に比べてより確実に行えるという長所を有する。

【図面の簡単な説明】

【図１】本発明の一実施の形態における管理基準作成システムの構成を示す構成図

【図２】同実施の形態におけるＳＴＢの内部構成を示す構成図

【図３】同実施の形態における管理装置の内部構成を示す構成図

【図４】同実施の形態におけるＳＴＢのデータ要求履歴情報記憶手段の記憶内容を説明する図

【図５】同実施の形態における管理装置の履歴情報記憶手段の記憶内容を説明する図

【図６】（ａ）：同実施の形態におけるＣＲＬ作成手段により作成されたＣＲＬを説明する図

（ｂ）～（ｃ）：同実施の形態における個別ＣＲＬ作成手段により作成された個別ＣＲＬを説明する図

【図７】別の実施の形態におけるＳＴＢの内部構成を示す構成図

【図８】同実施の形態における管理装置の内部構成を示す構成図

【図９】（ａ）：同実施の形態におけるＶＴＲ装置が登録される以前の、新規登録装置一覧情報記憶手段の記憶

20

内容を説明するための図

（ｂ）：同実施の形態におけるＶＴＲ装置が登録された後の、新規登録装置一覧情報記憶手段の記憶内容を説明するための図

【図１０】（ａ）～（ｂ）：不正・正規判定情報作成手段により作成された、不正・正規判定情報の個別リストを説明する図

【図１１】（ａ）：図１０（ａ）に示す判定結果の個別リストが送信される以前の、不正・正規情報格納手段における格納内容を示す図

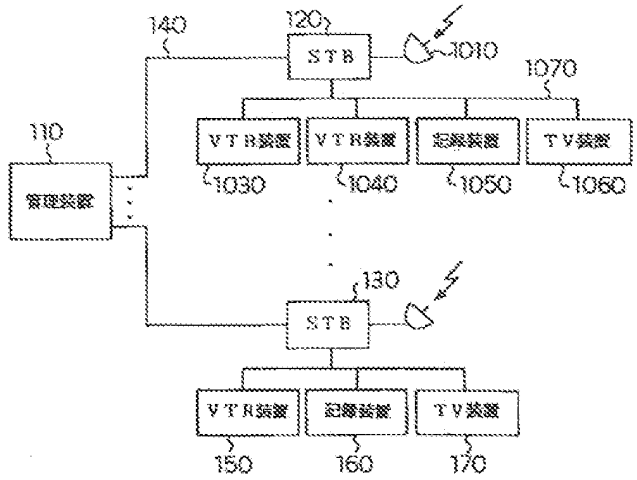
（ｂ）：図１０（ａ）に示す判定結果の個別リストが送信された後の、不正・正規情報格納手段における格納内容を示す図

【図１２】従来の専用受信機と端末装置との接続状況及び構成を示すブロック図

【符号の説明】

１１０	管理装置
１２０	第１ＳＴＢ
１３０	第ｎＳＴＢ
１５０、１０３０、１０４０	ＶＴＲ装置
１６０、１０５０	記録装置
１７０、１０６０	ＴＶ装置
１０１０	アンテナ

【図１】

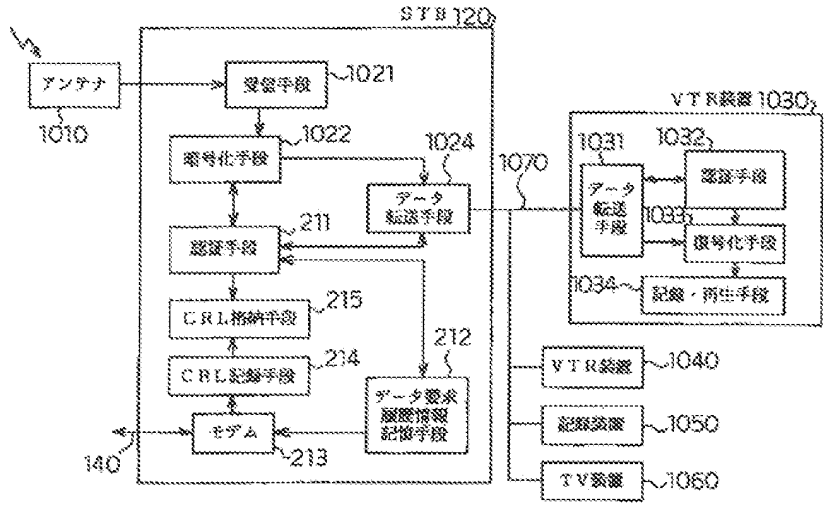


【図４】

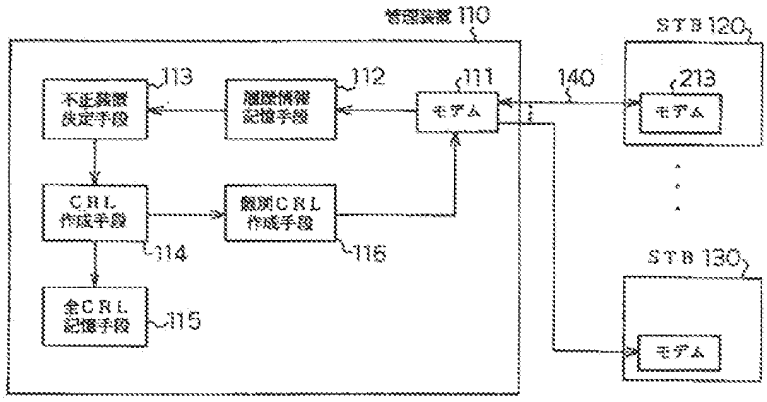
401

端末装置のEUI64	時刻情報
31060	1998年1月 1日12：00
11040	1998年1月 1日15：00
⋮	⋮
11030	1998年1月10日12：10
⋮	⋮
11040	1998年1月30日 7：00
21060	1998年1月31日23：00

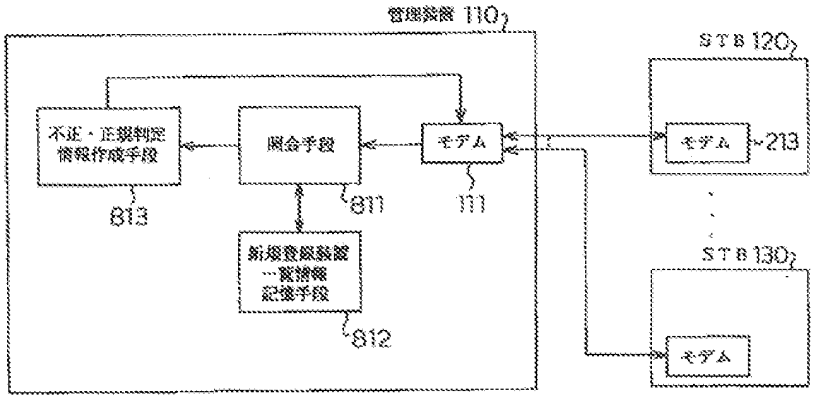
【図2】


STB 120
アンテナ
1010
受信手段
1021
暗号化手段
1022
データ転送手段
1024
認証手段
211
CRL格納手段
215
CRL記録手段
214
データ要求履歴情報記録手段
212
モデム
213
140
1070
VTR装置 1030
1031
データ転送手段
1032
認証手段
1033
暗号化手段
1034
記録・再生手段
VTR装置
1040
記録装置
1050
TV装置
1060

【図3】


管理装置 110
不正装置決定手段
113
履歴情報記録手段
112
モデム
111
140
CRL作成手段
114
最新CRL作成手段
116
全CRL記録手段
115
STB 120
213
モデム
STB 130
モデム

【図8】


管理装置 110
不正・正規判定情報作成手段
813
照合手段
811
モデム
111
新規登録装置一覧情報記録手段
812
STB 120
モデム
213
STB 130
モデム

【図5】

	501	502	503	504
	■■装置のEUI64	■■■■	■■■■	STBのEUI64
511	11030	1998年1月 1日11:00	■■のNさんの■■番号	90130
	31060	1998年1月 1日12:00	北海道のAさんの■■番号	90120
521	11040	1998年1月 1日15:00	北海道のAさんの■■番号	90120
	⋮	⋮	⋮	⋮
512	11030	1998年1月10日12:00	■■のNさんの■■番号	90130
513	11030	1998年1月10日12:10	北海道のAさんの■■番号	90120
	⋮	⋮	⋮	⋮
	20160	1998年1月30日10:00	■■のNさんの■■番号	90130
522	11040	1998年1月30日 7:00	北海道のAさんの■■番号	90120
	31050	1998年1月31日23:00	北海道のAさんの■■番号	90120

【図6】

(a)

	601
■■装置のEUI64	STBのEUI64
11030	90130
11030	90120

(b)

■■装置のEUI64	STBのEUI64
11030	90130

(c)

■■装置のEUI64	STBのEUI64
11030	90120

【図9】

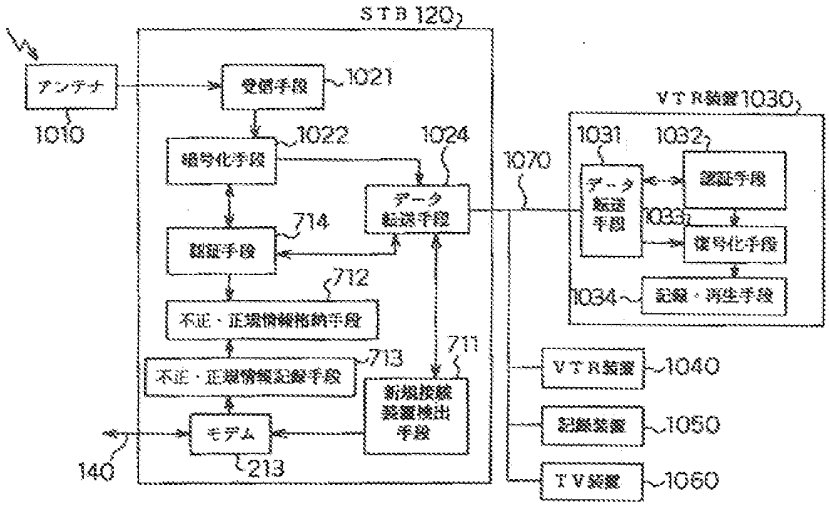
(a)

	■■■■装置のEUI64	STBのEUI64	■■
901	11030	90130	
	31060	90120	
	11040	90120	
	31050	90120	
	20160	90130	
	30170	90130	

(b)

			903
	■■■■装置のEUI64	STBのEUI64	■■
901	11030	90130	不正
	31060	90120	
	11040	90120	
	21050	90120	
	20160	90130	
	30170	90130	
902	11030	90120	不正

【図7】



【図10】

(a)

101

登録端末装置のEUI64	STBのEUI64	判定結果
11030	80130	不正

(b)

登録端末装置のEUI64	STBのEUI64	判定結果
11030	80120	不正

【図11】

(a)

登録端末装置のEUI64	判定結果
31060	正規
11040	正規
21050	正規

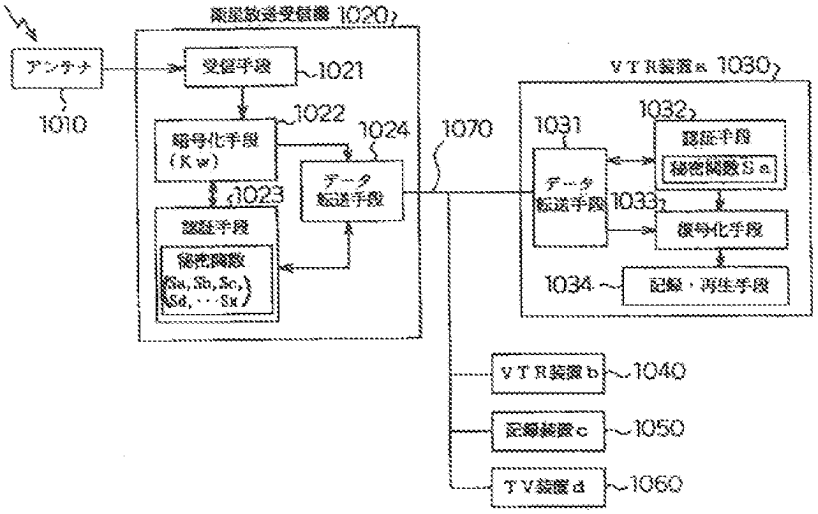
(b)

1112　　1111

登録端末装置のEUI64	判定結果
31060	正規
11040	正規
21050	正規
11030	不正

1113

【図１２】



フロントページの続き

(72)発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器
産業株式会社内